John Oliver, Chandler, AZ
Current DoD TS, SCI eligible
https://www.linkedin.com/in/johnoliver4
joliver@john-oliver.net

Technical pre-sales engineer / solutions architect with ten years directly supporting US Government customers as a badged tenant and seven in pre-sales roles.

Experience:

Mattermost (01/23 to 06/25)
Solutions Architect - Remote
Pre-sales engineer supporting federal sales team (DoD, IC, 4th estate, civilian agencies) to assist adoption of modern collaboration capabilities in US Government. Provide pre-sales technical expertise, conduct demonstrations and workshops, present at public-facing events and conferences to expand awareness of the many challenges and potential solutions. Part of team with >90% renewal rate and expansion of ARR by ~20% annually while closing two ~20,000 seat deals providing over $1M ARR each

Red Hat (09/17 to 01/23)
Sr. Solutions Architect - Remote
Pre-sales engineer for Red Hat portfolio (including RHEL, OpenShift, Ansible, etc.) for NAVWAR PEO C4I and various other US Navy commands. Communicate value of paid subscriptions to freely-available open-source software. Conduct presentations and workshops to drive adoption of modernization, agile/DevSecOps practices, containerization, automation, and cultural change within Navy programs.

SAIC (10/16 to 09/17)
Principal Systems Administrator at NIWC Pacific – San Diego, CA
UNIX SME & technical lead on effort to replace legacy naval messaging system with a virtualized Red Hat-based solution. Architect RHEL 7 based environment incorporating IdM, DNS, Splunk, SELinux to provide modern, supportable, secure services. Create jumpstart process for legacy Solaris-based product, kickstart for RHEL, and write Ansible playbooks and bash scripts to aid in virtualizing and reduce administrative time to install.

SAIC (07/12 to 10/16)
Principal Systems Administrator at NIWC Pacific – San Diego, CA
Lead systems administrator for nation-wide network consisting of Mac desktop clients and Linux servers. Technical lead for modernization of core infrastructure to a more manageable CentOS-based platform that supports current IA requirements and future growth. Extensive scripting to automate software deployment and patching, configuration management, hardening to STIG requirements, creation of STIG checklists, and implementation of IA policies. Employ pf and iptables firewall rulesets, SELinux to increase system security. Frequent contributor to internal and external working groups and community benchmarks.

Virginia Network Services (01/12 to 05/12)
Linux Systems Engineer – Chantilly, VA
Provided kickstart deployment tools, yum repositories, customized iptables rulesets, and syslog server configurations. Served as last-resort contact for outages on production systems running Apache web and application servers under RHEL 3 & 5, both physical and virtualized under VMware ESX.

FGM, Inc. (10/10 to 01/12)
Network Engineer at National Reconnaissance Office – Chantilly, VA
Packaged Windows applications for unattended installs for deployment via SCCM, AppV application virtualization, Windows batch files, Active Directory Group Policy Objects, testing, documentation of procedures, and engineered "back out" solutions for each delivery.

FGM, Inc. (12/08 to 09/10)
Linux Systems Engineer at NIWC Pacific – San Diego, CA
Sole administrator for RHEL 5 & Windows 2003 Server application servers running Tomcat, MySQL, MediaWiki, and some proprietary applications. Migrated all services to VMware-based virtualized environment. Built kickstart installers and shell scripts to automate configuration of new hosts. Responsible for maintaining patch levels and security posture of all lab systems.

Certification:
- Red Hat
    - RHCE – RHEL8 (verification code 160-099-008)
    - Red Hat Certified Specialist in Containers and Kubernetes
    - Red Hat Certified Specialist in OpenShift Administration
- Linux Foundation Kubernetes & Cloud Native Associate (cert # LF-5ztj5ee5i6)
- UCSD Extension UNIX Systems Administration
- CompTIA:
    - Linux+ - 27 APR 2010 (verification code 69K52GQJD34EQRJ2)
    - Security+ - 22 MAR 2013 (verification code MM2YJHCDJK4Q1F2G)
    - Network+ - 05 JAN 2000 (verification code QR7XY3JCRCREY77D)